September 9, 2010

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

Re: Interoperability Showing Supplement for San Francisco Bay Area Urban Area PS Docket No. 06-229

Redacted for Public Inspection

Dear Ms. Dortch:

The following information is intended to supplement the San Francisco Bay Area Urban Area's "interoperability showing" that is a condition of the waiver issued to authorize construction of a public safety broadband network on 700 MHz frequencies.

The San Francisco Bay Area Urban Area requests confidential treatment of some of the information contained in this letter. Pursuant to Section 0.459 of the Commission's rules, materials can be deemed confidential and withheld from public inspection if they meet any of the criteria of Section 0.457. In this case, information related to network performance, reliability, and priority access detailed in sections 2-4 below falls within Exemption 4 of the Freedom of Information Act ("FOIA") as it contains "trade secrets and commercial or financial information obtained from a person and privileged or confidential." This confidential information is redacted in the version being submitted for public viewing. A non-redacted version that includes this information will be provided to Ms. Jennifer Manner, Deputy Bureau Chief of the Commission's Public Safety and Homeland Security Bureau.

1. *Framework for nationwide priority access.*

On July 19, 2010, Motorola, Inc. submitted comments in PS Docket No. 06-229 responding to the Public Notice soliciting comment on Interoperability, Out Of Band Emissions, and Equipment Certification For 700 MHz Public Safety Broadband Networks. Motorola's proposal for a priority access framework is discussed on pages 13-17 of those comments.

2. *Link budget parameters and assumptions.*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. ***System design targets for physical layer over-the-air data rates.***

[redacted]

4. ***Static ICIC usage in the system design tools.***

[redacted]

5. ***S9 interface and Local Breakout roaming configuration.***

In reference to section A.5.6 of the San Francisco Bay Area Urban Area Interoperability filing, which is reproduced below, it should be noted that the BayWEB network will support local breakout, as well as the S9 interface. The filing reflects the current view on the applicability of local breakout with respect to existing Public Safety applications. The BayWEB network will support future applications that require Local Break Out.

A.5.6 Roaming Configurations

BayWEB will support home routed roaming configuration. Home routed configuration is when a user's traffic is routed back to the home network to enable the use of home applications and Internet access. The home routed case can support the majority of Public Safety applications and use cases. Home routed bearer flows benefit from QoS policies controlled in the home network. In addition, home routed provides many operational and security benefits, such as:

- *Single point of authentication for applications*
- *Single point for firewall, intrusion detection/prevention, and anti-virus protection*
- *Activity logging and Internet access policy control*

BayWEB will also support local breakout roaming configuration as needed for Public Safety applications. Local breakout configuration is when a user's traffic is routed within the visited network, and therefore is not routed back to the user's home network. Local breakout provides for optimization of bearer routing and access to visited network services. It should be noted that roamers may be subject to QoS policies of the local (i.e., visited) network. This is because 3GPP R8 standards allow the visited network to override QoS parameters from the home network. For this reason, the local services provided in the visited network are likely to be limited to IP services with static QoS and priority (e.g., best effort) for roaming users. It should be noted that the S9 interface is only applicable to local breakout scenarios. The S9 interface is used to provide dynamic charging and QoS policies from the home network to the visited network. Since use of local breakout scenarios are expected to be limited to static QoS policy, use of the S9 interface may not be required to support Public Safety applications. See section B for additional information regarding configurations used to support Public Safety applications.

Please contact me if there are any issues with this submission.

Sincerely,

Executive Director